



# CVE-2022-2056

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2022-2056
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@gitlab.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-06-30 16:15:00 UTC
<b>Updated</b>	2023-11-07 03:46:00 UTC
<b>Description</b>	Divide By Zero error in tiffcrop in libtiff 4.4.0 allows attackers to cause a denial-of-service via a crafted tiff file. For users that

## Risk And Classification

**Problem Types:** CWE-369

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	10.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	11.0	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	35	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	36	All	All	All
Application	<a href="#">Libtiff</a>	<a href="#">Libtiff</a>	4.4.0	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Active Iq Unified Manager</a>	-	All	All	All

## References

Reference	Source	Link	Tags
[SECURITY] Fedora 35 Update: libtiff-4.4.0-2.fc35 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
fix the FPE in tiffcrop (#415, #427, and #428) (!346) · Merge requests · libtiff / libtiff · GitLab	MISC	<a href="https://gitlab.com">gitlab.com</a>	
tiffcrop: FPE in computeOutputPixelOffsets, tiffcrop.c:5817 (#415) · Issues · libtiff / libtiff · GitLab	MISC	<a href="https://gitlab.com">gitlab.com</a>	
Debian -- Security Information -- DSA-5333-1 tiff	DEBIAN	<a href="https://www.debian.org">www.debian.org</a>	
[SECURITY] Fedora 36 Update: libtiff-4.4.0-2.fc36 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
[SECURITY] Fedora 36 Update: libtiff-4.4.0-2.fc36 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
June 2022 LibTIFF Vulnerabilities in NetApp Products   NetApp Product Security	CONFIRM	<a href="https://security.netapp.com">security.netapp.com</a>	
[SECURITY] Fedora 35 Update: libtiff-4.4.0-2.fc35 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	

[SECURITY] [DLA 3278-1] tiff security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>	
2022/CVE-2022-2056.json · master · GitLab.org / cves · GitLab	CONFIRM	<a href="https://gitlab.com">gitlab.com</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canon
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canon

### Vendor Comments And Credit

Discovery Credit

**LEGACY:** wangdw.augustus@gmail.com

### Legacy QID Mappings

<a href="#">160390</a> Oracle Enterprise Linux Security Update for libtiff (ELSA-2023-0095)
<a href="#">160411</a> Oracle Enterprise Linux Security Update for libtiff (ELSA-2023-0302)
<a href="#">181488</a> Debian Security Update for tiff (DLA 3278-1)
<a href="#">181520</a> Debian Security Update for tiff (DSA 5333-1)
<a href="#">183397</a> Debian Security Update for tiff (CVE-2022-2056)
<a href="#">198944</a> Ubuntu Security Notification for LibTIFF Vulnerabilities (USN-5619-1)
<a href="#">241054</a> Red Hat Update for libtiff (RHSA-2023:0095)
<a href="#">241120</a> Red Hat Update for libtiff (RHSA-2023:0302)
<a href="#">282943</a> Fedora Security Update for libtiff (FEDORA-2022-edf7301147)
<a href="#">282959</a> Fedora Security Update for libtiff (FEDORA-2022-b9c2a3a2b7)
<a href="#">296086</a> Oracle Solaris 11.4 Support Repository Update (SRU) 51.132.1 Missing (CPUOCT2022)
<a href="#">354326</a> Amazon Linux Security Advisory for libtiff : ALAS2022-2022-194
<a href="#">354588</a> Amazon Linux Security Advisory for libtiff : ALAS-2022-194
<a href="#">355159</a> Amazon Linux Security Advisory for libtiff : ALAS2023-2023-050
<a href="#">356138</a> Amazon Linux Security Advisory for libtiff : ALAS2-2023-2263
<a href="#">502794</a> Alpine Linux Security Update for tiff
<a href="#">503030</a> Alpine Linux Security Update for tiff
<a href="#">503131</a> Alpine Linux Security Update for tiff
<a href="#">505944</a> Alpine Linux Security Update for tiff
<a href="#">672155</a> EulerOS Security Update for libtiff (EulerOS-SA-2022-2443)

672204 EulerOS Security Update for libtiff (EulerOS-SA-2022-2469)
672462 EulerOS Security Update for libtiff (EulerOS-SA-2022-2850)
672464 EulerOS Security Update for libtiff (EulerOS-SA-2022-2825)
672478 EulerOS Security Update for libtiff (EulerOS-SA-2023-1039)
672508 EulerOS Security Update for libtiff (EulerOS-SA-2023-1014)
672526 EulerOS Security Update for libtiff (EulerOS-SA-2023-1128)
672539 EulerOS Security Update for libtiff (EulerOS-SA-2023-1104)
752422 SUSE Enterprise Linux Security Update for tiff (SUSE-SU-2022:2647-1)
752430 SUSE Enterprise Linux Security Update for tiff (SUSE-SU-2022:2648-1)
902423 Common Base Linux Mariner (CBL-Mariner) Security Update for libtiff (10025)
902427 Common Base Linux Mariner (CBL-Mariner) Security Update for libtiff (10007)
902624 Common Base Linux Mariner (CBL-Mariner) Security Update for libtiff (10007-1)
902685 Common Base Linux Mariner (CBL-Mariner) Security Update for libtiff (10025-1)
940871 AlmaLinux Security Update for libtiff (ALSA-2023:0095)
940898 AlmaLinux Security Update for libtiff (ALSA-2023:0302)
960525 Rocky Linux Security Update for libtiff (RLSA-2023:0302)
960537 Rocky Linux Security Update for libtiff (RLSA-2023:0095)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status [status.cve.report](#)**